Elements of Algebraic Structures January 23 2024

Lecture 5: Groups: An introduction

Lecture: Sujata Ghosh *Scribe: Sai Srujan P*

1 Topics for this lecture

In this lecture, we shall talk about the following

1. Motivation: Matrices example
2. Groups
3. Subgroups

2 Motivation

Definition 2.1 ($M_n(\mathbb{R})$) *Set of $n \times n$ matrices with real entries*

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

where $a_{ij} \in \mathbb{R}$.

2.1 Set Operations

Now, let us consider two operations Addition(+) and Multiplication(.).

Before proceeding further, let us define certain properties.

Closure Property

A set A is closed under the operation $*$, if for all $a, b \in A$, the result of $a * b$ is also in A.

$$\forall\ a, b \in A, \quad a * b \in A$$

Associative Property

The operation $*$ is associative on A if

$$\forall\ a, b, c \in A, \quad (a * b) * c = a * (b * c)$$

Identity Element

There exists an identity element $e \in A$ such that, for all $a \in A$:

$$\exists\ e \in A \quad \ni \quad a * e = e * a = a \quad \forall a \in A$$

Inverse Element

For each element $a \in A$, there exists an inverse element $a^{-1} \in A$ i.e.

$$\forall\ a \in A, \quad \exists\ a^{-1} \in A \quad \ni a * a^{-1} = a^{-1} * a = e$$

Commutative Property

The operation $*$ is commutative on A if

$$\forall\ a, b \in A, \quad a * b = b * a$$

2.1.1 Addition(+)

Consider$(M_n(\mathbb{R}), +)$ and see whether each of the above properties hold:

1. **Closure**

   Yes, addition of 2 $n \times n$ matrices is an $n \times n$ matrix.

2. **Associative**

   Yes, since each $a_{ij} \in \mathbb{R}$ and $\mathbb{R}$ is associative under $+$.

3. **Identity**

   Yes, since $\exists\ 0 \in \mathbb{R}$ and set $a_{ij} = 0\ \forall\ i, j$.

4. **Inverse**

   Yes, since for any given $a\ \exists\ -a \in \mathbb{R}$ and set $a_{ij} = -a_{ij}\ \forall\ i, j$.

5. **Commutative**

   Yes, since $a + b = b + a\ \forall\ a, b \in \mathbb{R}$.

2.1.2 Addition(+)

Consider$(M_n(\mathbb{R}), \times)$ and see whether each of the above properties hold:

1. **Closure**

   Yes, multiplication of 2 $n \times n$ matrices is an $n \times n$ matrix.

2. **Associative**

   Yes, it can be easily verifiable from the definition of $A \times B$

3. **Identity**

   Yes, $\exists$ *Identity* I_n

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

   $i.e.\ a_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$

4. **Inverse**

   No, $\exists\ A^{-1} \ni A \times A^{-1} = A^{-1} \times A = I_n$ iff $|A\ |! = 0$.

5. **Commutative**

   No, if we take $n >= 2$
   For suppose take $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$
   Then $AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.
   Also, $BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.
   Here $AB \neq BA$, therefore not Commutative.

2.1.3 General Linear Group($GL_n(\mathbb{R})$)

Define

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A \text{ is invertible}\}$$

Q. Consider $A, B \in GL_n(\mathbb{R})$

- Would $A + B \in GL_n(\mathbb{R})$?

  No
  Explanation

  For any A, Consider $B = -A$

$$A + (-A) = 0 \notin GL_n\ \mathbb{R}$$

- Would $AB \in GL_n(\mathbb{R})$?

  Yes
  Explanation

  From the definition of Inverse above
  A matrix $A \in M_n(\mathbb{R})$ is said to be invertible iff

$$\exists\ B \in M_n(\mathbb{R})\ \textit{such that}\ AB = BA = I_n$$

Here B is the inverse of A.

Now, $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AA^{-1} = I_n$.

$\therefore$ AB is invertible whenever A, B are invertible, and $B^{-1}A^{-1}$ is the inverse of AB

Consider $(\mathbf{GL_n}(\mathbf{R}), \cdot)$. Let's check each of the properties defined above:

1. **Closure**:

   Yes (Explanation: Previous paragraph)

2. **Associative**:

   Yes,
   Since associativity with respect to '$\cdot$' holds for any 3 matrices,
   it also holds for $GL_n(\mathbb{R})$.

3. **Identity**:

   Yes,
   We can observe that I_n is the identity
   since, $AI_n = I_nA = A$ for any $A \in GL_n(\mathbb{R})$.

4. **Inverse**:

   Yes,
   From the definition of $GL_n(\mathbb{R})$, it holds for any $A \in GL_n(\mathbb{R})$.

5. **Commutative**:

   No,
   Since Matrices in general are not commutative with respect to '$\cdot$'.

3 Groups

Consider $(\mathbf{G}, *)$, where, $G \neq \phi$ and *:binary operation on G.

Definition 3.1 (Binary Operation) *A binary operation on a set S is*

$$\text{mapping } * : S \times S \to S$$
$$\ni \text{each } (a, b) \to a * b \text{ over } S$$

Definition 3.2 (Group) *We say that $(\mathbf{G}, *)$ is a Group if the following conditions hold:*

1. ***Associative:*** $\forall\ a, b, c \in G$, $(a * b) * c = a * (b * c) \in\ G$
2. ***Identity:*** *$\exists$ an element $e \in G \quad \ni \quad \forall a \in G$, $a * e = e * a = a$*
3. ***Inverse:*** *For each $a \in G, \exists\ a^{-1} \in G \quad \ni \quad a * a^{-1} = a^{-1} * a = e$*

Example *The following are a few examples.*

1. $(\mathbf{Z}, +)$ *forms a group*

   Here Identity: 0, *and Given* $a \in \mathbf{Z}$, $-a$ *is it's Inverse*

2. *Let* S *be any non-empty set, and let* $G = \{\rho : \rho \text{ is a bijection on } S\}$.
   Consider $(G, \circ)$, *where* $\circ$ *is the composition of two bijections.*
   Then, $(G, \circ)$ *forms a group.*

   We generally call it the symmetric group on S *and denote it by* $\mathbf{SG_3}$

   Consider $SG_{\{1,2\}} = (\{e, \tau\})$.

$$e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$\circ$	e	τ
e	e	τ
τ	τ	e

Composition table for S

   From the table above we see that for any $a, b \in SG_{\{1,2\}}$, $a \circ b = b \circ a$
   [Composition table is Symmetric].

$$\therefore SG_{\{1,2\}} \text{ a Commutative Group, denoted as } \mathbf{SG_2}$$

3. $SG_{\{1,2,3\}} = \mathbf{SG_3}$.
   The elements of SG_3*:*

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \tau &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ \tau' &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} & \tau'' &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \sigma' &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

Exercise *Composition Table for SG_3.*

$\circ$	e	τ	τ'	τ''	σ	σ'
e	e	τ	τ'	τ''	σ	σ'
τ	τ	e	τ''	σ'	τ'	σ
τ'	τ'	σ'	e	σ	τ''	τ
τ''	τ''	σ	σ'	e	τ	τ'
σ	σ	τ''	τ	τ'	σ'	e
σ'	σ'	τ'	σ	τ	e	τ'

***Composition table for* SG$_3$**

Is SG$_3$ Commutative? No

Consider τ'' *and* σ

$$\tau'' \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau$$

$$\sigma \circ \tau'' = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau^{'}$$

We can see that $\tau \circ \sigma \neq \sigma \circ \tau^{'}$.

Proposition 3.4 *$SG_n (n \geq 3)$ is not Commutative*

Proof. Consider $\tau_n^{''}$ and σ_n given by

$$\tau_n^{''}(i) = \begin{cases} \tau^{''}(i) & 1 \leq i \leq 3, \\ i & \text{otherwise.} \end{cases}$$

$$\sigma_e(i) = \begin{cases} \sigma(i) & 1 \leq i \leq 3, \\ i & \text{otherwise.} \end{cases}$$

$\implies \tau_n^{''} \circ \sigma_n \neq \sigma_n \circ \tau_n^{''}$ [From the above example]

Hence SG$_n (n \geq 3)$ is not Commutative

□

4 Subgroups

Definition 4.1 (Subgroup) *Given $(G, \cdot)$ and $H \subseteq G$*
H is called a subgroup of G if H is itself a group under the operation of G
i.e., If the following properties hold:

1. *Closure: For all $a, b \in H$, $a \cdot b \in H$.*
2. *Identity Element: $\exists$ an element $e \in H$ such that for all $a \in H$, $a * e = e * a = a$*
3. *Inverse Element: For each $a \in H, \exists\ a^{-1} \in H$ such that $a * a^{-1} = a^{-1} * a = e$*

***Notation:* $\mathbf{H \leq G}$**

Proposition 4.2 (Two-step Subgroup test) *Let $(G, *)$ be a group and $H \subseteq G$. Then $H \leq G$ if and only if:*

1. *$\forall\ a, b$, $a * b \in H$*
2. *$\exists$ Identity $e \in H$*
3. *For all $a \in H$, $a^{-1} \in H$.*

Exercise: Prove that

1. $e_H = e_G$
2. $h_H^{-1} = h_G^{-1}$, for any $h \in H$]

Proof.

1. For any $h \in H$, we have

$$h \cdot e_G = e_G \cdot h = h$$
$$\text{Also, } h \cdot e_H = e_H \cdot h = h$$
$$\therefore e_G = e_H \text{ (As Cancellation Laws hold in G)}$$

2. For any $h \in H$, we have

$$h \cdot h_G^{-1} = h_G^{-1} \cdot h = e_G$$
$$\text{Also, } h_H^{-1} \cdot h = e_H = e_G \text{ (Part 1)}$$
$$\therefore h_H^{-1} = h_G^{-1} \text{ (As Cancellation Laws hold in G)}$$

$\square$

Example *Let's look at a few Examples*

1. *Subgroups of* SG_3

$$\{e\}, SG_3, \{e,\tau\}, \{e,\tau'\}, \{e,\tau"\}, \{e,\sigma,\sigma'\}$$

2. *Subgroup of* $GL_2(\mathbb{R})$

$$\left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{R}, ad \neq 0\right\}$$

3. *Subgroups of* $(\mathbb{Z}, +)$

$$\{e\}, 2\mathbb{Z}$$

Proposition 4.4 *Any subgroup of $(\mathbb{Z},+)$ is of the form $(m\mathbb{Z},+)$, for some $m \in \mathbb{Z}$.*

Proof.

$\Longleftarrow$ [$(m\mathbb{Z},+) \leq (\mathbb{Z},+)$ for any $m \in \mathbb{Z}$]

1. Consider arbitrary $x, y \in m\mathbb{Z}$

$$\begin{aligned} &x = mk \textit{ and } y = ml \text{ for some } k, l \in \mathbb{Z} \\ &\implies x + y = mk + ml \\ &= m(k+l) \in m\mathbb{Z} \textit{ as } k + l \in \mathbb{Z} \end{aligned}$$

$\therefore$ For any $x, y \in m\mathbb{Z}$, $x + y \in m\mathbb{Z}$.

2. $0 = m \cdot 0 \in m\mathbb{Z}$.

3. Consider an arbitrary $x \in m\mathbb{Z}$

$$\begin{aligned} &x = m(p) \text{ for some } p \in \mathbb{Z} \\ &-x = -mp = m(-p) \in m\mathbb{Z} \text{ as } -p \in \mathbb{Z} \\ &x \in m\mathbb{Z} \implies -x \in m\mathbb{Z} \text{ [Here } x + (-x) = 0] \end{aligned}$$

Thus, $(m\mathbb{Z},+)$ forms a subgroup of $(\mathbb{Z},+)$ [**Two-step Subgroup test**]

$\Longrightarrow$ [Any $(H,+) \leq (\mathbb{Z},+)$ is of the form $(m\mathbb{Z},+)$ for some $m \in \mathbb{Z}$]

- $H = \{0\}$, we are done

- Suppose $H \neq \{0\}$.
  Without loss of generality, assume H contains positive integers

  Suppose m' be the least positive integer in H
  [Existence of m' is guaranteed by Well-ordering principle]

  We know that $m'\mathbb{Z} \subset H$ [$\because H \leq (\mathbb{Z},+)$]

  Claim: $m'\mathbb{Z} = H$
  Proof by Contradiction

  Suppose not, i.e. $m'\mathbb{Z} \neq H$

  $$\implies \exists\, x \in H \ni x \notin m'\mathbb{Z}$$

  Now we have $x = m'y + r$, where $y, r \in \mathbb{Z}$ and $0 < r < m'$
  Also $m'y \in m'\mathbb{Z} \subset H$
  $\implies m'y \in H$ and $-m'y \in H$
  $\therefore x - m'y = x + (-m'y) \in H$ (As $x \in H$)

  So $r \in H$, but we see that $r < m'$

  This contradicts the fact that m' is the least positive integer in H

  $$\therefore m'\mathbb{Z} = H$$

$\square$